(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/046782 A3

(51) International Patent Classification⁷: G06F 1/00, G11B 20/00

(21) International Application Number: PCT/US00/42780

(22) International Filing Date:
13 December 2000 (13.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/464,724 16 December 1999 (16.12.1999) US

(71) Applicant: MICROSOFT CORPORATION [US/US]; One Microsoft Way, Redmond, WA 98052 (US).

(72) Inventor: ABBURI, Rajasekhar; 7844 NE 10th Street, Medina, WA 98039 (US).

(74) Agents: ROCCI, Steven, J. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th Floor, One Liberty Place, Philadelphia, PA 19103 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

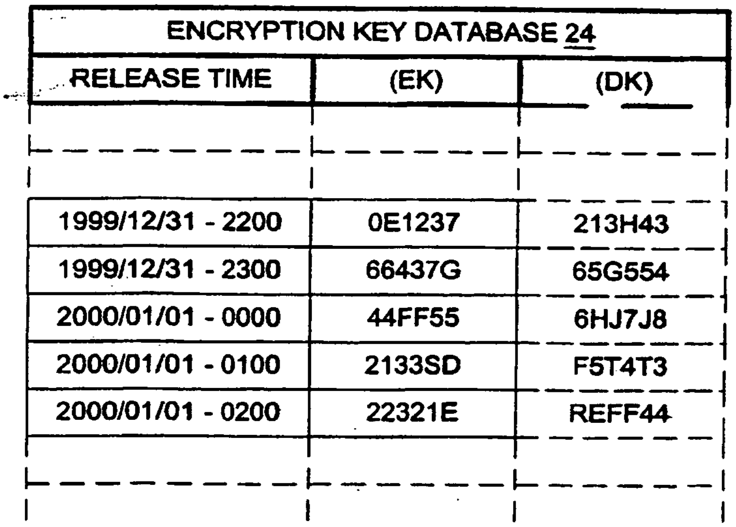
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
12 September 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF PRE-RELEASING ENCRYPTED DIGITAL DATA



ENCRYPTION KEY DATABASE 24		
RELEASE TIME	(EK)	(DK)
1999/12/31 - 2200	0E1237	213H43
1999/12/31 - 2300	66437G	65G554
2000/01/01 - 0000	44FF55	6HJ7J8
2000/01/01 - 0100	2133SD	F5T4T3
2000/01/01 - 0200	22321E	REFF44

(57) Abstract: A method for pre-releasing digital content is disclosed. A release time for the digital content is determined and the digital content is encrypted with an encryption key. The encrypted digital cotent is decryptable by a decryption key corresponding to the encryption key. The encrypted digital content is distributed to at least one content user prior to the release time, and the decryption key for the encrypted digital content is released to the content user at the release time. The content user may then decrypt the encrypted digital content with the released decryption key at or after the release time. The encryption key may be selected from an encryption key database having a plurality of entries, where each entry includes a release time for releasing a piece of digital content, and an encryption key for encrypting the digital content that is to be released at the release time.

INTERNATIONAL SEARCH REPORT

Intei nal Application No
PCT/US 00/42780

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11B H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 857 020 A (PETERSON JR MENDEL LAZEAR) 5 January 1999 (1999-01-05) column 3, line 33 - line 44 column 4, line 20 -column 5, line 42 ---	1-5, 11-14, 21,22, 24,28,29
A	US 5 703 951 A (DOLPHIN JANET L) 30 December 1997 (1997-12-30) abstract; figures 4,8,9,14,16 column 6, line 11 - line 42 column 10, line 8 - line 29 column 11, line 33 -column 13, line 17 -----	1,6-10, 13, 15-21, 30-53

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 13 June 2002	Date of mailing of the international search report 20/06/2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Sigolo, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 00/42780

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5857020 A	05-01-1999	AU 7616596 A	27-06-1997
		WO 9721162 A1	12-06-1997
		US 5825876 A	20-10-1998
US 5703951 A	30-12-1997	US 5457746 A	10-10-1995
		US 5677953 A	14-10-1997
		AU 694742 B2	30-07-1998
		AU 7687494 A	03-04-1995
		EP 0719485 A1	03-07-1996
		IL 110891 A	12-03-1999
		JP 9503322 T	31-03-1997
		WO 9508231 A1	23-03-1995

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 June 2001 (28.06.2001)

PCT

(10) International Publication Number
WO 01/46782 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/US00/42780

(22) International Filing Date:
13 December 2000 (13.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/464,724 16 December 1999 (16.12.1999) US

(71) Applicant: MICROSOFT CORPORATION [US/US]; One Microsoft Way, Redmond, WA 98052 (US).

(72) Inventor: ABBURI, Rajasekhar; 7844 NE 10th Street, Medina, WA 98039 (US).

(74) Agents: ROCCI, Steven, J. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th Floor, One Liberty Place, Philadelphia, PA 19103 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF PRE-RELEASING DIGITAL CONTENT AND ENCRYPTION KEY DATABASE FOR USE THEREWITH

ENCRYPTION KEY DATABASE 24

RELEASE TIME	(EK)	(DK)
1999/12/31 - 2200	0E1237	213H43
1999/12/31 - 2300	66437G	65G554
2000/01/01 - 0000	44FF55	6HJ7J8
2000/01/01 - 0100	2133SD	F5T4T3
2000/01/01 - 0200	22321E	REFF44

(57) Abstract: A method for pre-releasing digital content is disclosed. A release time for the digital content is determined and the digital content is encrypted with an encryption key. The encrypted digital cotent is decryptable by a decryption key corresponding to the encryption key. The encrypted digital content is distributed to at least one content user prior to the release time, and the decryption key for the encrypted digital content is released to the content user at the release time. The content user may then decrypt the encrypted digital content with the released decryption key at or after the release time. The encryption key may be selected from an encryption key database having a plurality of entries, where each entry includes a release time for releasing a piece of digital content, and an encryption key for encrypting the digital content that is to be released at the release time.

WO 01/46782 A2

Title of the Invention

Method of Pre-Releasing Digital Content and Encryption Key Database for Use Therewith

Technical Field

The present invention relates to a framework for pre-releasing digital content in an encrypted form. More specifically, the present invention relates to selecting a release time for the digital content, encrypting the content with an encryption key, pre-releasing the encrypted content selected prior to the release time, and releasing the encryption key at the release time.

Background of the Invention

In many instances, it is desirable to set a release time for releasing information to the relevant public, thereby preventing such relevant public from obtaining and/or accessing and/or using such information until such release time. For example, in the recording industry, it is typical that a new recording by an artist (a musical artist or group, e.g.) is not released to the purchasing public until a selected release time.

Reasons for use of such a release time are many and varied. For example, such release time may be employed as a marketing technique to generate interest or 'buzz' in connection with the to-be-released information (e.g., a new recording by a musical artist, a video copy of a motion picture for home playback) prior to the release time. As another example, the release time is necessary to ensure that all interested information-seekers have relatively equal access to the information (e.g., the latest government employment statistics, the latest quarterly report for a publicly held corporation) at the same time. Accordingly, no particular information-seeker can obtain an advantage over any other information-seeker by obtaining such information first. In still another example, an information supplier may be contractually or otherwise legally bound not to release the information until the release time. Of course, many other reasons for employing release times exist.

Oftentimes, the use of a release time in connection with to-be-released information either intentionally or unintentionally results in the creation of a pent-up demand for such information. As should be understood, such created demand for such information 'bursts forth' at the release time, and the information supplier may be unable to immediately satisfy such demand at the release time, at least initially.

In the situation where such information is electronically distributed in a digital form as digital content over a communications network such as the Internet or the like, for example, it is oftentimes the case that too many requesters are requesting the information / digital content from too few content servers. In such situation, it may also be the case that the communications network itself does not have the capacity or 'bandwidth' to handle the volume of uploading requests for the digital content and/or to handle the volume of downloading digital content. As should be understood, wait times for obtaining the digital content in such a situation can be excessive. As should also be understood, such situation is exacerbated as the size of the downloading digital content increases.

More importantly, such a situation may result in a first digital-content-seeker being provided with the digital content well before a second merely because the second had a longer wait time than the first. Similarly, it may be the case that the first digital-content-seeker can download the digital content over a relatively faster access link and the second can only download the information over a relatively slower access link. In either instance, issues of fairness arise in that the first digital-content-seeker can obtain an advantage over the second by having the digital content first. Notably, such issues of fairness arise in spite of the use of a release time, as was discussed above.

Accordingly, a need exists for a method of allowing an information-seeker, and particularly a digital-content-seeker, to obtain access to information / digital content at a release time without undue delay, regardless of the size of the digital content or the speed of the access link through which the digital content is obtained.

Summary of the Invention

The aforementioned need is satisfied by the present invention which comprises a method for pre-releasing digital content, wherein a release time for the digital content is determined and the digital content is encrypted with an encryption key. The encrypted digital content is decryptable by a decryption key corresponding to the encryption key. The encrypted digital content is distributed to at least one content user prior to the release time, and the decryption key for the encrypted digital content is released to the content user at the release time. The content user may then decrypt the encrypted digital content with the released decryption key at or after the release time. In one embodiment of the present invention, the encryption key is selected from an encryption key database having a plurality of entries, where each entry includes a release time for releasing a piece of digital content, and an encryption key for encrypting the digital content that is to be released at the release time.

As should be understood, the decryption key is generally much smaller in size than the encrypted digital content. Accordingly, such decryption key may be downloaded or otherwise obtained relatively quickly. Moreover, since the encrypted information may be downloaded or otherwise obtained over an extended period of time prior to the release time, bandwidth issues, wait time issues, size of the digital content issues, access speed issues, and other similar issues as discussed above are minimized if not eliminated, and most any digital-content-seeker can obtain access to digital content at the release time thereof without undue delay.

Brief Description of the Drawings

The forgoing summary, as well as the following detailed description of embodiments of the present invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention there are shown in the drawings embodiments which are presently preferred. As should be understood, however, the invention is not limited to the precise arrangements and instrumentalities shown. In the drawings:

Fig. 1 is a block diagram representing a general purpose computer system in which aspects of the present invention and/or portions thereof may be incorporated;

Fig. 2 is a flow diagram showing steps performed both by a content provider in pre-releasing digital content (left side) and a content user in obtaining pre-released digital content (right side) in accordance with one embodiment of the present invention;

Fig. 3 is a block diagram of an encryption key database that may be employed in accordance with one embodiment of the present invention;

Figs. 4A and 4B are block diagrams showing encrypted content distributed from a content provider to a content user in accordance with embodiments of the present invention; and

Fig. 5 is a block diagram representing various elements employed to release the encryption key to a content user in accordance with embodiments of the present invention.

Detailed Description of the Invention

Referring now to Fig. 1, the following discussion is intended to provide a brief general description of a suitable computing environment in which the present invention and/or portions thereof may be implemented. Although not required, the invention is described in the general context of computer-executable instructions, such as program modules, being executed by a computer, such as a client workstation or a server. Generally, program modules include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. Moreover, it should be appreciated that the invention and/or portions thereof may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. The invention may further be practiced in connection with the system and method disclosed in co-pending and commonly assigned U.S. Patent Application No. 09/290,363, entitled "ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT" and filed on April 12, 1999, hereby incorporated by reference.

As shown in Fig. 1, an exemplary general purpose computing system includes a conventional personal computer 120 or the like, including a processing unit 121, a system memory 122, and a system bus 123 that couples various system components including the system memory to the processing unit 121. The system bus 123 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read-only memory (ROM) 124 and random access memory (RAM) 125. A basic input/output system 126 (BIOS), containing the basic routines that help to transfer information between elements within the personal computer 120, such as during start-up, is stored in ROM 124.

The personal computer 120 may further include a hard disk drive 127 for reading from and writing to a hard disk (not shown), a magnetic disk drive 128 for reading from or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading from or writing to a removable optical disk 131 such as a CD-ROM or other optical media. The hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive interface 133, and an optical drive interface 134, respectively. The drives and their associated computer-readable media provide non-volatile storage of computer readable instructions, data structures, program modules and other data for the personal computer 20.

Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 129, and a removable optical disk 131, it should be appreciated that other types of computer readable media which can store data that is accessible by a computer may also be used in the exemplary operating environment. Such other types of media include a magnetic cassette, a flash memory card, a digital video disk, a Bernoulli cartridge, a random access memory (RAM), a read-only memory (ROM), and the like.

A number of program modules may be stored on the hard disk, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including an operating system 135, one or more application programs 136, other program modules 137 and program data 138. A user may enter commands and information into the personal computer 120 through input devices such as a keyboard 140 and pointing device 142. Other input devices (not shown) may include a microphone, joystick, game pad, satellite disk, scanner, or the like. These and other input devices are often connected to the processing unit 121 through a serial port interface 146 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port, or universal serial bus (USB). A monitor 147 or other type of display device is also connected to the system bus 123 via an interface, such as a video adapter 148. In addition to the monitor 147, a personal computer typically includes other peripheral output devices (not shown), such as speakers and printers. The exemplary system of Fig. 1 also includes a host adapter 155, a Small Computer System Interface (SCSI) bus 156, and an external storage device 162 connected to the SCSI bus 156.

The personal computer 120 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 149. The remote computer 149 may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the personal computer 120, although only a memory storage device 150 has been illustrated in Fig. 1. The logical connections depicted in Fig. 1 include a local area network (LAN) 151 and a wide area network (WAN) 152. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

When used in a LAN networking environment, the personal computer 120 is connected to the LAN 151 through a network interface or adapter 153. When used in a WAN networking environment, the personal computer 120 typically includes a modem 154 or other means for establishing communications over the wide area network 152, such as the Internet. The modem 154, which may be internal or external, is connected to the system bus 123 via the serial port interface 146. In a networked environment, program modules depicted relative to the personal computer 120, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

Referring now to Figs. 2 through 5, wherein like numerals are used to indicate like elements throughout, there is shown in Fig. 2 a method of pre-releasing digital content (left side), and also a method of obtaining digital content (right side) in accordance with embodiments of the present invention. In the methods, a content provider 10 intending to distribute digital content 12 to a content user 14 (Figs. 4A and 4B) first determines a content release time (TR) for the content 12 (step 201 in Fig. 2). Such content release time (TR) may be any appropriate time; for example, the time (TR) may be 12 midnight, 1 a.m., 9:30 a.m., 12 noon, 6:37 p.m. on a particular day, etc. If desirable, the time (TR) may be specified with finer or coarser granularity.

With a determined release time (TR), the content provider 10 then encrypts the content 12 (content (C) in Fig. 2) with a selected encryption key (EK) (step 203), and distributes the encrypted content (EK(C)) prior to the content release time (TR) (step 205). Concomitant with the distribution of the encrypted content (EK(C)) (step 205), such distributed encrypted content (EK(C)) is received by a content user 14 (step 209). Notably, the present invention does not require that the release time (TR) be determined before the content (C) is encrypted with the encryption key (EK) unless the selection of the encryption key (EK) is based on the release time (TR), as will be described below. The encryption key (EK) may be any appropriate encryption key, and may be employed in connection with any appropriate encryption algorithm.

In one embodiment of the present invention, the encryption key (EK) is part of an asymmetric key pair that includes a decryption key (DK) as will be described below. As will be evident from the discussion that follows, the encryption key (EK) and the decryption key (DK) are akin to a public key and a private key, respectively, although the decryption key (DK) is to be made public at the release time (TR). The encryption key (EK) may alternatively be a symmetric key, wherein the decryption key (DK) is the encryption key (EK). However, in the event that the encryption key (EK) is to be publicly disclosed prior to the release time (TR), as will be discussed below, it should be evident that such encryption key (EK) should not in fact be a symmetric key.

The encrypted content (EK(C)) may be distributed (step 205) by the content provider 10 and received by the content user 14 (step 209) by any available means before the content release time (TR). In one embodiment of the present invention, the content provider 10 distributes and the content user 14 receives the encrypted content (EK(C)) over a communications network such as the Internet or the like. However, the encrypted content (EK(C)) may also be distributed by other means, including by way of an optical disk, a magnetic disk, or tape; by way of direct transmission from the content provider 10 to the content user 14; by way of an electronic bulletin board, by way of electronic mail; by way of regular mail; by way of an Internet web page; etc. Moreover, the actual process of distribution and receipt of the encrypted content (EK(C)) from the content provider 10 to the content user 14 may occur by way of several intermediate distribution steps; may be based on a request from the content user 14 to the content provider 10 or to an intermediary; or may be automatically delivered from a content provider 10 or an intermediary to the content user 14. Payment for receiving the encrypted content (EK(C)) may occur, or may not be necessary.

Preferably, the distribution of the encrypted content (EK(C)) occurs a sufficient amount of time prior to the content release time (TR) (i.e., with a sufficient amount of 'lead time') such that such distribution can occur in a relatively orderly manner, with little if any difficulty encountered by a content user 14 when attempting to access a server or the like to obtain the encrypted content (EK(C)). Any amount of lead time may be employed, although it is to be appreciated that more lead time should ideally be provided when demand for a particular piece of content 12 is expected to be high. As should be appreciated, if it is anticipated that 100,000 content users 14 will wish to pre-release download a new computer game, 100 days of lead time will provide an average of 1,000 downloads per day, while 10 days of lead time will provide an average of 10,000 downloads per day.

A longer lead time is of course desirable since necessary bandwidth is reduced. However, a longer lead time also increases the probability that a nefarious individual will determine how to decrypt the encrypted content (EK(C)) prior to the release time (TR). Of course, a shorter lead time is acceptable provided the distribution mechanism has sufficient available bandwidth to support the higher download frequency. At any rate, a lead time of a month or more could be desirable for distributing relatively high demand content 12 having a relatively large size, such as for example a 60 minute recording by a popular musical performer, and a lead time of a week or so could be desirable for distributing relatively high demand content 12 having a relatively small size, such as for example a quarterly forecast for frozen orange juice concentrate from the U.S. Department of Agriculture.

When the encrypted content (EK(C)) is received by a content user, whether it occurs before or after the content release time (TR) (step 209), the content user 14 preferably stores such received encrypted content (EK(C)) in an appropriate storage mechanism. Any such appropriate storage mechanism may be employed; for example, the mechanism may be a magnetic disk or tape, an optical disk, a hard drive, RAM, ROM, etc. As should be understood, the content 12 encrypted as (EK(C)) is intended to be played back or rendered, ultimately, on an appropriate playback or rendering device. Depending on the encrypted content (EK(C)) (text, music, video, multimedia, a database, plotting data, etc.), the playback / rendering device may include or be embodied by a personal computer, a portable personal appliance, a digital video monitor, an audio digital playback system, etc.

As should be understood, the decryption key (DK) for decrypting the encrypted content (EK(C)) is released to the content user 14 only at or after the content release time (TR) (step 207, Fig. 2). Accordingly, such content user 14 can receive such content decryption key (DK) at or some time after the content release time (TR) (step 211). As with the distribution of the encrypted content (EK(C)), the decryption key (DK) may be released by any appropriate means; for example, the decryption key (DK) may be released by being made generally available on a server or the like. Alternatively, the decryption key (DK) may be sent to a content user 14 by way of an Internet web page, an electronic mail message, a regular mail message, or the like.

In one embodiment of the present invention, the decryption key (DK) is released to the content user 14 over a communications network such as the Internet or the like. However, like the encrypted content (EK(C)), the decryption key (DK) may also be released by other means, including by way of an optical disk, a magnetic disk, or tape; by way of direct transmission from the content provider 10 to the content user 14; by way of an electronic bulletin board, by way of electronic mail; by way of regular mail; by way of an Internet web page; etc. Moreover, and also like the encrypted content, the actual process of releasing the decryption key (DK) to the content user 14 may occur by way of several intermediate releasing steps; may be based on a request from the content user 14 to a key source 16 (Fig. 5) or to an intermediary thereof; or may be automatically delivered from the key source 16 or an intermediary to the content user 14. Notably, and as discussed in more detail below, the key source 16 is not necessarily the content provider 10.

Of course, the content user 14 may attempt to obtain the decryption key (DK) from the key source 16 prior to the content release time (TR), although such attempt should fail. In particular, the key source 16 is trusted not to release the decryption key (DK) for the encrypted content (EK(C)) until the content release time (TR).

Since the release of the decryption key (DK) for the encrypted content (EK(C)) occurs at the content release time (TR), and since it is possible that large numbers of content users 14 will wish to obtain the decryption key (DK) immediately thereafter, it is possible that a small delay can occur in connection therewith. As should be understood, though, the decryption key is generally much smaller in size than the encrypted digital content. Accordingly, an undue delay should not occur, with little if any difficulty encountered by a content user 14 when attempting to access a server or the like to obtain the decryption key (DK) for the encrypted content (EK(C)).

It is to be noted that although the encrypted content (EK(C)) is distributed before the content release time (TR), and although the content decryption key (DK) for such encrypted content (EK(C)) is not released until the release time (TR), a content user 14 may receive the encrypted content (EK(C)) after the release time (TR), and/or may also receive the decryption key (DK) after the release time (TR). Moreover, since it is expected that a content user 14 may wish to obtain the decryption key (DK) for some time after the release time (TR), the key source is expected to provide such decryption key (DK) for at lease a minimum period of time after the release time (TR).

In the course of obtaining the decryption key (DK) from a key source, and in one embodiment of the present invention, a content user 14 may have appropriate hardware and/or software that automatically detects from received encrypted digital content (EK(C)) where the decryption key for such content is located (e.g., a web address for a key source 16 / server or the like) and may also automatically obtain such decryption key (DK) from the decryption key location when such decryption key (DK) is available. In such a situation, it may be preferable to package the encrypted digital content (EK(C)) with information on the key source 16 for obtaining the decryption key (DK). Likewise, it may be preferable to package the encrypted digital content (EK(C)) with the content release time (TR), as is seen in Fig. 4A (omitted in Fig. 4B).

In one embodiment of the present invention, a content user 14 obtains the decryption key (DK) from the key source 16 in exchange for a payment. Accordingly, and as seen in Fig. 5, the key source 16 may include or be associated with a payment device 18 for obtaining a payment from the content user 14 in exchange for sending the decryption key (DK) to such content user 14. Such payment device 18 may be any appropriate payment device, including a credit payment device, a debit payment device, a cash payment device, a charge payment device, or the like. Typically, the payment device 18 receives a credit, debit, or charge account number from the content user 14 and electronically charges the payment against an account associated with such number.

As also seen in Fig. 5, the key source 16 may also include or be associated with a sending and/or releasing device 20 for sending / releasing the private key (DK) to the content user 14. Such sending / releasing device 20 may be any appropriate device; for example, the device 20 may send an Internet web page, an electronic mail message, a regular mail message, etc. with the private key (DK) to the content user 14.

As further seen in Fig. 5, the key source 16 may include or be associated with a receive device 22 for receiving a request for the decryption key (DK) from the content user 14. The receive device 22 may be any appropriate device. Typically, the receiving device 22 receives an Internet web page or request from the content user 14, an electronic mail message from the content user 14, or the like.

Once the key source 16 has received a request for the decryption key (DK) from the content user 14 by way of a receive device 22 (if necessary), has processed a payment by way of the payment device 18 (if necessary), and has sent the decryption key (DK) by way of the send/release device 20 to the content user 14 such content user receives the decryption key (DK) (step 211 in Fig. 2) and may then store the received decryption key (DK) in an appropriate location. Such appropriate location will vary depending upon the application and the location of the corresponding encrypted content (EK(C)), and may include long-term storage (e.g., a hard drive) if the decryption key (DK) does not immediately decrypt the encrypted digital content (EK(C)) or short-term storage (e.g., RAM) if the decryption key (DK) immediately decrypts the encrypted digital content (EK(C)). Generally, any appropriate storage location may be employed. Thereafter, the content user 14 may then employ the decryption key (DK) to decrypt the encrypted digital content (EK(C)) (step 213 in Fig. 2), thereby resulting in the content 12 in an unencrypted form. Such content 12 may then be rendered by an appropriate rendering device and/or stored in the decrypted form.

Referring now to Fig. 3, in one embodiment of the present invention, the content provider 10 obtains the encryption key (EK) from an encryption key database 24 that has a plurality of entries, where each entry includes a release time (TR) and a corresponding encryption key (EK). As should be understood, for each entry in the encryption key database 24, the encryption key (EK) for such entry is for encrypting content 12 that is to be released at the release time (TR) of such entry. For example, then, when a content provider 10 wishes to release a piece of content 12 at a release time (TR) of December 31, 1999, at 11:00 p.m. (1999/12/31 – 2300), such content provider 10 refers to the entry in the encryption key database 24 having such release time (TR), as seen in Fig. 3, which in this case has a corresponding encryption key (EK) of 66437G, and employs such encryption key (EK) to encrypt the content 12.

In one embodiment of the present invention, each entry of the encryption key database 24 also includes a corresponding decryption key (DK) that corresponds to the encryption key (EK). Accordingly, and as also seen in Fig. 3, for a piece of content 12 encrypted to be released at a release time (TR) of December 31, 1999 at 11:00 p.m. (1999/12/31 - 2300) and therefore encrypted with the encryption key (EK) of 66437G, the corresponding decryption key (DK) is 65G554.

Preferably, the release times (TR) in the plurality of entries in the encryption key database 24 are regularly temporally spaced. Accordingly, and as seen in Fig. 3, hourly release times (TR) are provided, i.e. on December 31, 1999 at 10:00 p.m. (1999/12/31 - 2200), at 11:00 p.m. (1999/12/31 - 2300), at midnight (2000/01/01 - 0000), on January 1, 2000 at 1:00 a.m.(2000/01/01 - 0100), etc. Of course, entries may be other than hourly; for example, the periodicity of each entry may be daily, semi-daily, bi-daily, every 27 minutes, every 8.5 hours, etc. Preferably, each release time (TR) is with respect to a particular time zone or an absolute time – for example, Eastern U.S. time, coordinated universal time (UTC), etc.

If desired, the content provider 10 may release each decryption key (DK) at the corresponding release time (TR). Accordingly, such content provider 10 can access each decryption key (DK) in the encryption key database 24. Alternatively, a third party may be responsible for releasing each encryption key (DK) at the appropriate release time (TR). In such a situation, the third party may construct the encryption key database 24 and publish such database 24 to the world with each release time (TR) and with each corresponding encryption key (EK), but without each corresponding decryption key (DK). Of course, the content provider 10 can also construct and publish the database 24 without the decryption keys (DK).

Of course, the actual release of the decryption key (DK) at the release time (TR) may not in fact take place exactly at such release time (TR). For example, such actual release may be delayed for any of a variety of reasons. Whether or not the release of a decryption key (DK) for a release time (TR) actually takes place at such release time (TR), the important point is that the actual release of such decryption key (DK) does not take place before such release time (TR). Accordingly 'at the release time' and variations thereof may be interpreted to include 'no earlier than the release time' and corresponding variations thereof without departing from the spirit and scope of the present invention.

Thus, any content provider 10 may consult such encryption key database 24 to select an encryption key (EK) based on a pre-selected release time (TR). Even though such content provider 10 does not know the decryption key (DK) that corresponds to such encryption key (EK) for such release time (TR), it is not necessary that such content provider 10 have knowledge of such decryption key (DK). Such content provider 10 need only encrypt the content 12 with the selected encryption key (EK), and then rely on the third party to release the corresponding decryption key (DK) at the corresponding release time (TR).

In one embodiment of the present invention, the content provider 10 encrypts the content 12 a single time with an encryption key (EK) from the encryption key database 24, as is seen in Fig. 4A. Thus, only one decryption key (DK) (released at the corresponding release time (TR) is necessary to decrypt the encrypted content. In another embodiment of the present invention, the content provider 10 encrypts the content 12 a plurality of times with a plurality of encryption keys (EK) from the encryption key database 24, as is seen in Fig. 4B (with two encryptions). Accordingly, a content user 14 must obtain each corresponding decryption key (DK) to decrypt the encrypted content. As should be understood, the release time (TR) corresponding to each encryption key (EK) must be no later than the determined release time (TR) for the content 12. As should also be understood, multiple layers of encryption, as seen in Fig. 4B, protect against accidental early release of the content 12 should one of the corresponding decryption keys (DK) be accidentally or nefariously released early.

In one embodiment of the present invention, the content provider 10 chooses the encryption key (EK) from one of several available encryption key databases 24. In particular, although it is to be understood that only a single such database 24 is necessary, it may be useful for administrative or security purposes to have multiple such databases 24. For example, one database 24 may provide encryption keys (EK) for finance-oriented content, while another database 24 may provide encryption keys (EK) for entertainment-oriented comment. Likewise, in a manner akin to that shown in Fig. 4B, encryption keys (EK) for the same or different release times (TR) may be selected from different databases 24 for purposes of multiple layers of encryption.

Of course, in any instance where an encryption key (EK) may have originated from one of multiple databases 24, it is necessary to include a reference to the particular database 24 with the encrypted content 12. Accordingly, such particular database 24 is identified and may be accessed by a content user 14 at the appropriate release time (TR) to obtain the decryption key (DK) corresponding to the encryption key (EK). If the database 24 is to be accessed on a network such as an intranet or the Internet, the reference is preferably a network address through which the database 24 can be accessed.

The programming necessary to effectuate the processes performed in connection with the present invention is relatively straight-forward and should be apparent to the relevant programming public. Any particular programming, then, may be employed to effectuate the present invention.

In the foregoing description, it can be seen that the present invention comprises a new and useful method of pre-releasing and obtaining digital content, and also an encryption key database 24 for use therewith. With such method and database 24, an information-seeker, and particularly a digital-content-seeker, can obtain access to information / digital content at a release time without undue delay, regardless of the size of the digital content or the speed of the access link through which the digital content is obtained. Importantly, in the present invention, each encryption key database is generally expected to be published by a well known trusted party which may or may not be different from the content publishers, and is expected to be distributed widely. Each decryption key (DK) is to be made broadly available at its specified time (TR), but not any sooner. It should be appreciated that changes could be made to the embodiments described above without departing from the invention concepts thereof. It should be understood, therefore, that this invention is not limited to the particular embodiments disclosed, but it is intended to cover modifications within the spirit and scope of the present invention as defined by the appended claims.

CLAIMS

1. A method of pre-releasing digital content having a predetermined release time, the method comprising:

encrypting the digital content with an encryption key, the encrypted digital content being decryptable by a decryption key corresponding to the encryption key;

distributing the encrypted digital content to at least one content user prior to the release time;

releasing the decryption key for the encrypted digital content to the content user at the release time, wherein the content user can then decrypt the encrypted digital content with the released decryption key.

2. The method of claim 1 wherein the releasing step comprises sending the decryption key to the content user.

3. The method of claim 2 wherein the releasing step comprises sending the decryption key to the content user by way of a device selected from a group consisting of an Internet web page, an electronic mail message and a regular mail message.

4. The method of claim 1 wherein the encrypting step comprises encrypting the digital content with an encryption key from an asymmetric key pair.

5. The method of claim 1 wherein the encrypting step comprises encrypting the digital content with an encryption key that is a symmetric key, wherein the decryption key is the encryption key.

6. The method of claim 1 wherein the encrypting step

comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time and an encryption key, the encryption key being selected from one of the entries in the database based on the release time of the entry and the determined release time of the digital content.

7. The method of claim 6 wherein the encrypting step comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time and an encryption key, the release times in the plurality of entries being regularly temporally spaced.

8. The method of claim 7 wherein the encrypting step comprises encrypting the digital content a plurality of times with a plurality of encryption keys from the encryption key database, the release time corresponding to each encryption key being no later than the determined release time for the digital content.

9. The method of claim 6 wherein the encrypting step comprises encrypting the digital content a plurality of times with a plurality of encryption keys selected from a plurality of encryption key databases.

10. The method of claim 6 wherein the encrypting step comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time, an encryption key, and a corresponding decryption key.

11. The method of claim 1 further comprising providing the decryption key for at least a minimum period of time after the release time.

12. The method of claim 11 further comprising packaging the encrypted digital content with the release time.

13. A method of pre-releasing digital content having a pre-determined release time, the method comprising:

encrypting the digital content with an encryption key, the encrypted digital content being decrypt-able by a decryption key corresponding to the encryption key; the decryption key not being released to the content user until the release time; and

distributing the encrypted digital content to at least one content user prior to the release time, wherein the content user cannot decrypt the encrypted digital content until the decryption key is released at the release time.

14. The method of claim 13 wherein the encrypting step comprises encrypting the digital content with an encryption key from an asymmetric key pair.

15. The method of claim 13 wherein the encrypting step comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time and an encryption key, the encryption key being selected from one of the entries in the database based on the release time of the entry and the determined release time of the digital content.

16. The method of claim 15 wherein the encrypting step comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time and an encryption key, the release times in the plurality of entries being regularly temporally spaced.

17. The method of claim 16 wherein the encrypting step comprises encrypting the digital content a plurality of times with a plurality of encryption keys from the encryption key database, the release time corresponding to each encryption key being no later than the determined release time for the digital content.

18. The method of claim 15 wherein the encrypting step comprises encrypting the digital content with an encryption key selected from an encryption key database having a plurality of entries, each entry including a release time, an encryption key, and a corresponding decryption key.

19. The method of claim 15 wherein the encrypting step comprises encrypting the digital content a plurality of times with a plurality of encryption keys selected from a plurality of encryption key databases.

20. The method of claim 15 further comprising packaging the encrypted digital content with the release time.

21. A method of obtaining digital content having a predetermined release time, the method comprising:

firstly receiving prior to the release time the digital content encrypted according to an encryption key associated with the release time, the encrypted digital content being decrypt-able by a decryption key corresponding to the encryption key;

secondly receiving at the release time the decryption key for the encrypted digital content; and

decrypting the encrypted digital content with the released decryption key.

22. The method of claim 21 wherein the second receiving

step comprises obtaining the decryption key from a key source.

23. The method of claim 21 wherein the second receiving step comprises automatically detecting from the received encrypted digital content where the decryption key is located, and automatically obtaining such decryption key when available.

24. The method of claim 21 wherein the second receiving step comprises obtaining the decryption key from a key source in exchange for a payment.

25. The method of claim 21 wherein the second receiving step comprises obtaining the decryption key from a key source selected from a group consisting of an Internet web page and an electronic bulletin board.

26. The method of claim 21 wherein the second receiving step comprises receiving the decryption key by way of a device selected from a group consisting of an Internet web page, an electronic mail message and a regular mail message.

27. The method of claim 21 wherein the first receiving step comprises firstly receiving prior to the release time the digital content encrypted a plurality of times according to a plurality of encryption keys, each encryption key associated with a particular release time, the release time associated with each encryption key being no later than the predetermined release time for the digital content.

28. The method of claim 21 wherein the first receiving step comprises receiving the encrypted digital content packaged with the release time.

29. The method of claim 28 wherein the second receiving step comprises automatically obtaining the decryption key at the release time.

30. An encryption key database having a plurality of entries, each entry including:

a release time for releasing a piece of digital content; and

an encryption key for encrypting the digital content that is to be released at the release time, the encrypted digital content being distributed to at least one content user prior to the release time.

31. The database of claim 30 wherein each entry further includes a corresponding decryption key for decrypting the encrypted digital content, the decryption key for being released to the content user at the release time, wherein the content user can then decrypt the encrypted digital content with the released decryption key.

32. The database of claim 30 wherein the release times in the plurality of entries are regularly temporally spaced.

33. A piece of digital content encrypted a plurality of times with a plurality of encryption keys from the encryption key database of claim 30, the release time corresponding to each encryption key being no later than the determined release time for the digital content.

34. The encrypted digital content of claim 33 packaged with the release time.

35. A piece of digital content encrypted a plurality of times with a plurality of encryption keys from a plurality of the encryption key databases of claim 30.

36. The encrypted digital content of claim 30 packaged with the release time.

37. In combination with the database of claim 30, a sending device for sending the decryption key to the content user.

38. The sending device of claim 37 comprising a member of the group consisting of an Internet web page sending device and an electronic mail sending device.

39. In combination with the database and the sending device of claim 37, a payment device for obtaining a payment from the content user in exchange for sending the decryption key to the content user.

40. In combination with the database of claim 30, a receiving device for receiving a request for the decryption key from the content user.

41. The receiving device of claim 40 comprising a member of the group consisting of an Internet web page receiving device and an electronic mail receiving device.

42. The database of claim 30 wherein the encryption key and the decryption key are an asymmetric key pair.

43. The database of claim 30 wherein the encryption key and the decryption key are the same key.

44. A computer-readable medium having stored thereon a data structure having a plurality of entries, each entry including:

a first data field containing data representing a release time for releasing a piece of digital content;

a second data field containing data representing an encryption key for encrypting the digital content that is to be released at the release time, the encrypted digital content being distributed to at least one content user prior to the release time.

45. The medium of claim 44 wherein each entry further includes a third data field containing data representing a corresponding decryption key for decrypting the encrypted digital content, the decryption key for being released to the content user at the release time, wherein the content user can then decrypt the encrypted digital content with the released decryption key.

46. The medium of claim 45 wherein the encryption key in the second data field and the decryption key in the third data field are the same key.

47. The medium of claim 44 wherein the release times in the first data fields of the plurality of entries are regularly temporally spaced.

48. In combination with the medium of claim 44, a sending device for sending the decryption key to the content user.

49. The sending device of claim 48 comprising a member of the group consisting of an Internet web page sending device and an electronic mail sending device.

50. In combination with the medium and the sending device of claim 48, a payment device for obtaining a payment from the content user in exchange for sending the decryption key to the content user.

51. In combination with the medium of claim 44, a receiving device for receiving a request for the decryption key from the content user.

52. The receiving device of claim 51 comprising a member of the group consisting of an Internet web page receiving device and an electronic mail receiving device.

53. The medium of claim 44 wherein the encryption key and the decryption key are an asymmetric key pair.

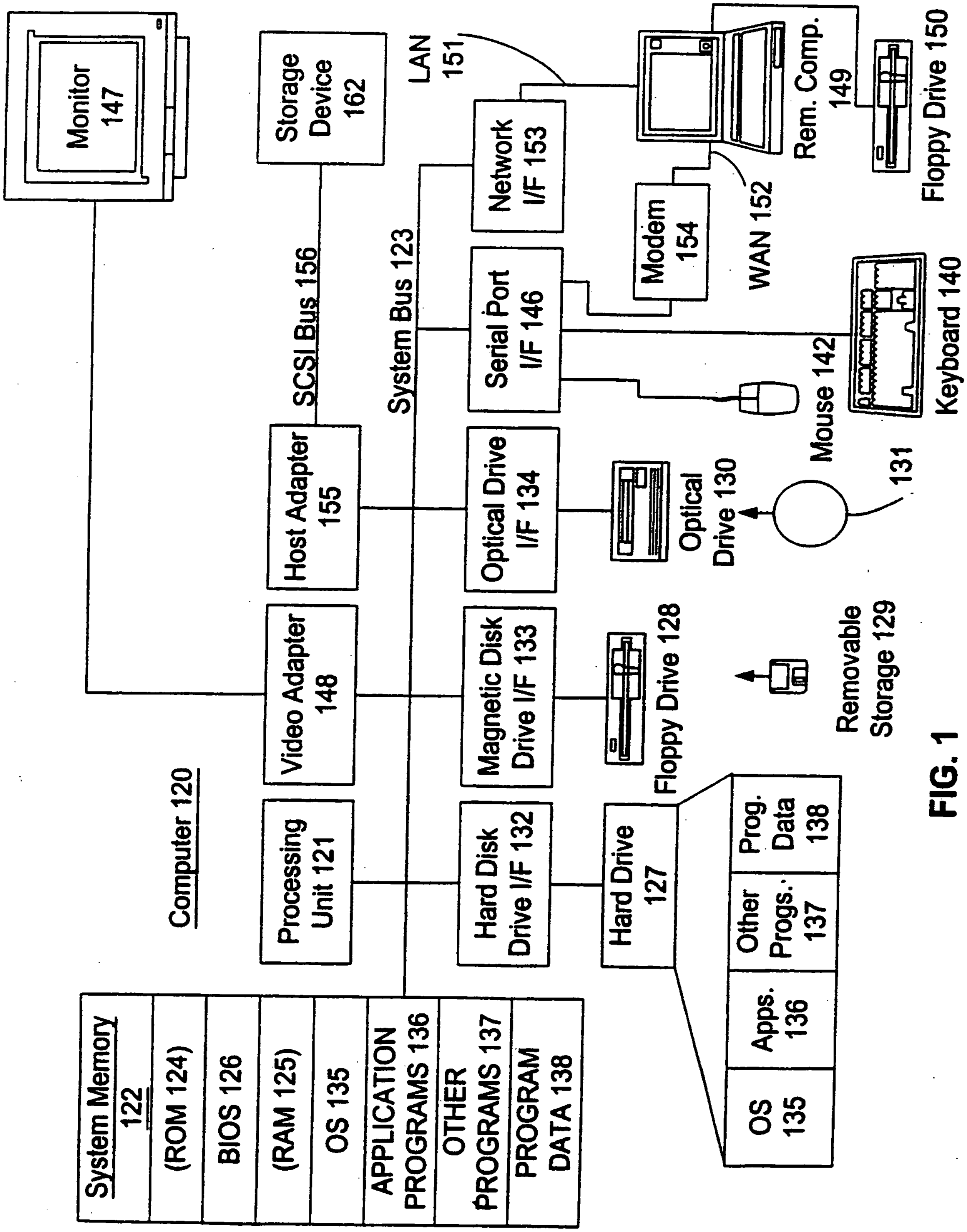

Monitor 147
Storage Device 162
LAN 151
Rem. Comp. 149
Floppy Drive 150
Network I/F 153
WAN 152
Modem 154
SCSI Bus 156
System Bus 123
Serial Port I/F 146
Keyboard 140
Mouse 142
Host Adapter 155
Optical Drive I/F 134
Optical Drive 130
131
Video Adapter 148
Magnetic Disk Drive I/F 133
Floppy Drive 128
Removable Storage 129
Computer 120
Processing Unit 121
Hard Disk Drive I/F 132
Hard Drive 127
Prog. Data 138
Other Progs. 137
Apps. 136
OS 135
System Memory 122
(ROM 124)
BIOS 126
(RAM 125)
OS 135
APPLICATION PROGRAMS 136
OTHER PROGRAMS 137
PROGRAM DATA 138

FIG. 1

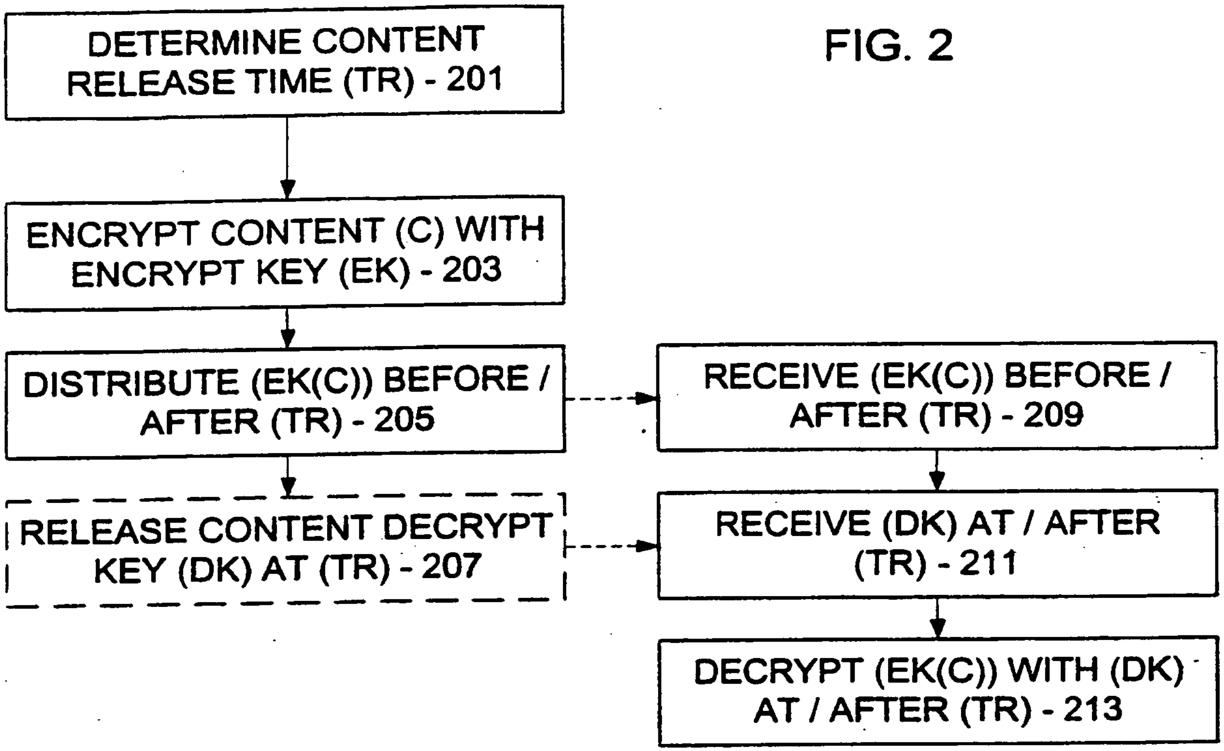

DETERMINE CONTENT RELEASE TIME (TR) - 201
ENCRYPT CONTENT (C) WITH ENCRYPT KEY (EK) - 203
DISTRIBUTE (EK(C)) BEFORE / AFTER (TR) - 205
RELEASE CONTENT DECRYPT KEY (DK) AT (TR) - 207
RECEIVE (EK(C)) BEFORE / AFTER (TR) - 209
RECEIVE (DK) AT / AFTER (TR) - 211
DECRYPT (EK(C)) WITH (DK) AT / AFTER (TR) - 213

FIG. 2

ENCRYPTION KEY DATABASE 24

RELEASE TIME	(EK)	(DK)
1999/12/31 - 2200	0E1237	213H43
1999/12/31 - 2300	66437G	65G554
2000/01/01 - 0000	44FF55	6HJ7J8
2000/01/01 - 0100	2133SD	F5T4T3
2000/01/01 - 0200	22321E	REFF44

FIG. 3

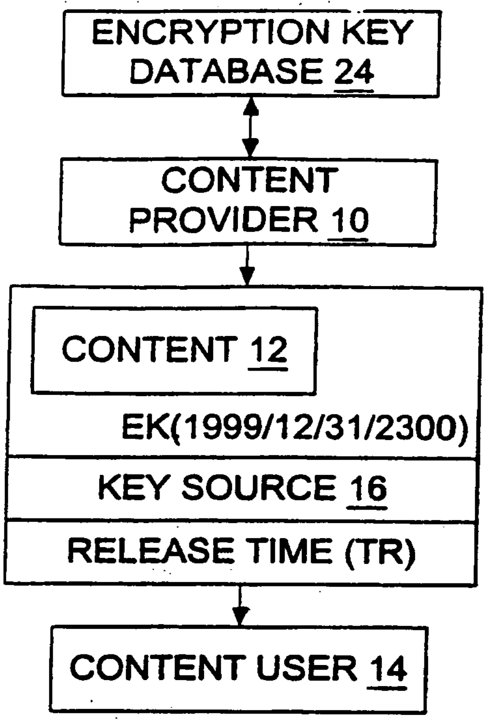


FIG. 4A

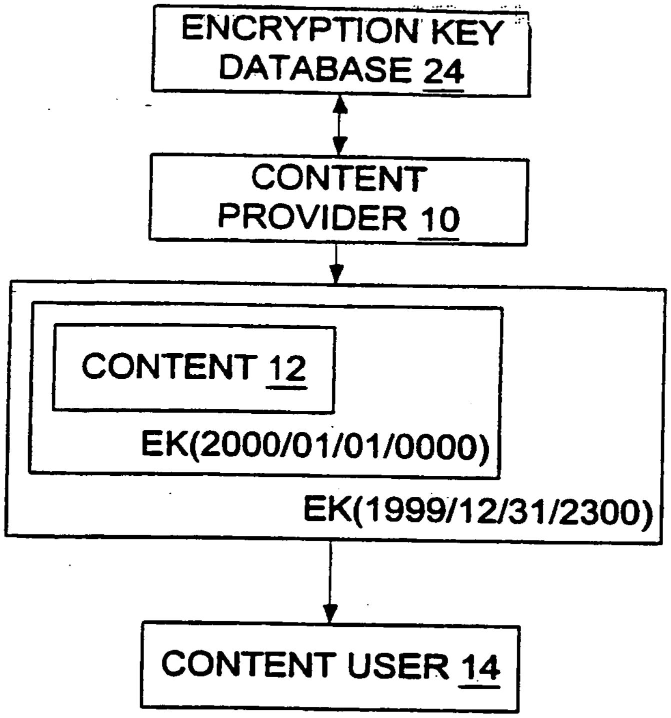


FIG. 4B

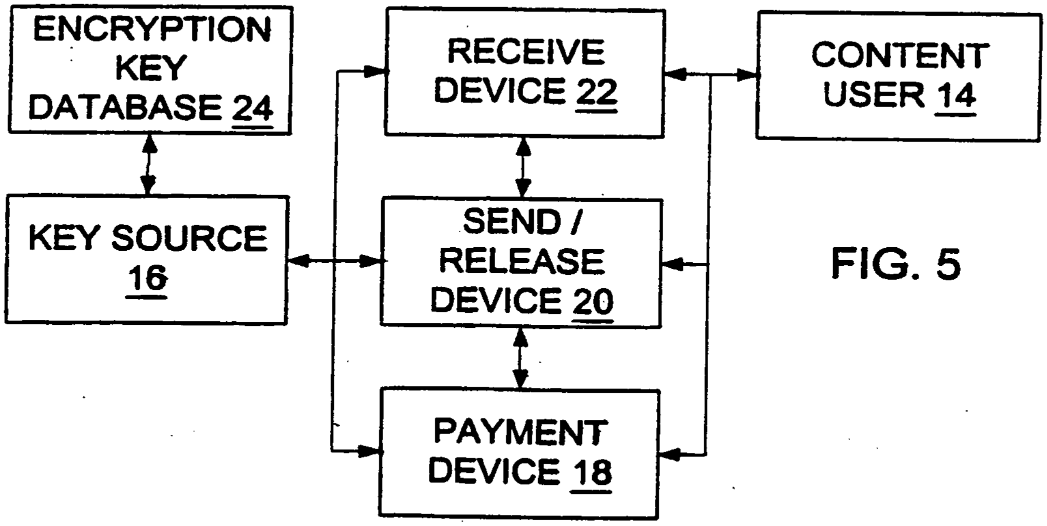


FIG. 5